United States Military Academy
West Point, New York 10996

A FRAMEWORK FOR THE ANALYSIS OF THE FUTURE COMBAT SYSTEM CONCEPTUAL DESIGN ALTERNATIVES

OPERATIONS RESEARCH CENTER
TECHNICAL REPORT 01-05-1

Major Michael J. Kwinn, Jr, Ph.D.
Analyst, Operations Research Center

Lieutenant Colonel Mark J. Davis
Director, Operations Research Center

Colonel Michael L. McGinnis, Ph.D.
Professor and Head, Department of Systems Engineering

30 April 2001

The Operations Research Center is supported by the Assistant Secretary of the Army (Financial Management)

REPORT DOCUMENTATION PAGE			*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
30 April 2001	Tech	7/1/00 to 6/30/01

4. TITLE AND SUBTITLE

A Framework for the analysis of the future combat system conceptual design alternatives

5a. CONTRACT NUMBER n/a

5b. GRANT NUMBER n/a

5c. PROGRAM ELEMENT NUMBER n/a

6. AUTHOR(S)

Major Michael J. Kwinn, Jr., Ph.D.
Lieutenant Colonel Mark J. Davis

5d. PROJECT NUMBER n/a

5e. TASK NUMBER n/a

5f. WORK UNIT NUMBER n/a

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Operations Research Center of Excellence
Department of Systems Engineerig
United States Military Academy
West Point, New York 10996

8. PERFORMING ORGANIZATION REPORT NUMBER 01-05-1

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

PM Future Combat Systems

10. SPONSOR/MONITOR'S ACRONYM(S) PM FCS

11. SPONSOR/MONITOR'S REPORT NUMBER(S) n/a

12. DISTRIBUTION/AVAILABILITY STATEMENT

Distribution Statement A - Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

n/a

14. ABSTRACT

The United States Army is frenetically engaged in an ambitious initiative to transform itself from a Cold War legacy force into a new millennium force, the Objective Force, designed to dominate potential enemies through the first half of the new century. The centerpiece of this transformed Army will be the Future Combat System (FCS). The common expectation of this transformed force is that it will derive its dominance over potential rivals by taking full advantage of a potential Revolution in Military Affairs (RMA) anchored in a host of current and near-future technological advances. Our research presents a more mature understanding of what may ultimately comprise the next RMA and offers a model of battlefield information functional design that can guide FCS system design and that of the Objective Force overall.

15. SUBJECT TERMS

FCS - Future Combat Systems

16. SECURITY CLASSIFICATION OF: a. REPORT	b. ABSTRACT	c. THIS PAGE	17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
					LTC Mike Kwinn, Jr.
					19b. TELEPHONE NUMBER *(Include area code)*
n/a	n/a	n/a	SAR	60	845-938-5591

A FRAMEWORK FOR THE ANALYSIS OF THE FUTURE COMBAT SYSTEM CONCEPTUAL DESIGN ALTERNATIVES

Lead Analyst
Major Michael J. Kwinn, Jr., Ph.D.
Analyst, Operations Research Center

A TECHNICAL REPORT
OF THE
OPERATIONS RESEARCH CENTER
UNITED STATES MILITARY ACADEMY

Directed by
Lieutenant Colonel Mark J. Davis
Director, Operations Research Center

Approved by
Colonel Michael L. Mc Ginnis, Ph.D.
Professor and Head, Department of Systems Engineering

30 April 2001

About the Author

MAJOR MICHAEL J. KWINN, JR. is an Analyst in the Operations Research Center at the United States Military Academy (USMA), West Point, New York. He received a BS from USMA in 1984, an MS in Systems Engineering from the University of Arizona in 1994 and a Ph.D. in Management Science and Information Systems from the University of Texas at Austin in 2000. His research interests are personnel management systems, future combat systems analysis and force structure analysis through the use of optimization and simulation models.

Acknowledgments

I would like to acknowledge the Office of the Program Manager, Future Combat System for supporting this research. I would also like to I would also like to acknowledge some individuals who helped in the development of this approach and analysis:

Mr. Dan Pierson, Chief, Systems Methodology, Office of the PM, FCS. Dan gave me tremendous access and insight into the FCS program. This was critical in my understanding of an undertaking in an area that I was not completely familiar. His input and confidence in my abilities were an inspiration. I look forward to future collaborative research efforts with his office.

Lieutenant Colonel (Promotable) Mark J. Davis, director of the Operations Research Center of Excellence. LTC Davis provided me with a great deal of the focus for this research and the development of this framework. He patiently guided me, and directed me, through its development. He also helped convert this from my thoughts into a readable document. Successful completion of this project would not have been possible without his assistance and communication abilities.

Major Ricardo Morales, Major Mark Brantley and Major Barry Ezell, fellow analysts in the Operations Research Center of Excellence. My fellow analysts listened to my ranting and quietly provided me with insights and support. Their reviews and assistance were invaluable.

Major Jamie Fischer, Assistant Professor in the Department of History, USMA. Jamie provided the analysis for the historical references to the Revolution in Military Affairs for this report.

Table of Contents

Executive Summary

In this report, we present a framework for the analysis of the conceptual design alternative for the Future Combat System (FCS). We focus our discussion by identifying that in Network-centric Warfare (NCW) that will provide militaries with a Revolution in Military Affairs (RMA). We chose this approach to ensure that the FCS provides the US Army with the greatest potential leap in capabilities allowed through the application of current and near-term technological innovations.

Through readings and descriptions intended to define what constitutes a RMA, especially relying on the definitions provided by the Office of Net Assessment lead by Andrew Marshall, we assert that a RMA can only occur in an environment where three preconditions are satisfied. First, there must be a fundamental change in the nature of warfare, usually, but not necessarily, through the application of technological advances. Second, there must be associated doctrinal innovation that employs these advances in novel and significant ways. Third, there must be organizational acceptance of the combination of both the technology and the doctrinal innovations.

We propose that the fundamental change in the nature of warfare in a network-centric force occurs in the Engagement Process. The five steps in this process in a platform-centric force, Search/Detect, Identify, Target/Track, Engage and Assess become Battlefield Information Functions (BIFs) in a network-centric force.

These BIFs form the information requirements to enable collaborative engagement capabilities to the force. It is in this collaborative engagement capability that

the FCS can achieve its dominance on the future battlefield. As such, we discuss the capabilities and associated metrics within each of these functions required to leverage the potential of network-centric operations and, thereby achieve the RMA.

We continue with a discussion of some of the associated doctrinal innovations necessary to satisfy the second precondition of the RMA. These focus on the potential changes in fire control measures and the changes in command structures that require further analysis to support the changes in warfare.

The final precondition for a RMA is organizational acceptance. This may be the most difficult precondition to satisfy. To this end we issue two specific mandates to the analytical community. The first mandate is to the Modeling and Simulation community. They must appropriately and completely model new systems (under design), specifically the distributed collaborative information operations capability envisioned by the Objective Force designers. Modification of existing simulations will not sufficiently prove the increased capabilities of the networked force. The second mandate is to the analytical and academic communities. These resources must address the specific capabilities of the Objective Force and detail how to achieve those capabilities. This will serve to reduce the speculation and supposition that typifies current operational discussions and reduces confidence in the success of the initiative.

1. Introduction

The United States Army, at the direction of the General Eric K. Shinseki the Chief of Staff, is in the midst of a transformation effort that may become the largest and most significant research and development undertaking since the atomic bomb. The single, overriding purpose behind this massive effort is to change the current Army structure into an Objective Force concept destined to keep the United States military in its current dominant world position through the first half of the new century. The centerpiece of this transformation initiative is the Future Combat System (FCS). There are four contractor teams, or consortiums, developing competing conceptual design alternatives for this "system of systems".

The challenge for the government team is to develop a set of measures to fairly assess each of the conceptual designs and chose the few that will be further developed for the next phase of the FCS acquisition process. The problem faced by the government team in this effort is that most of the typical metrics and evaluation methods previously relied on in acquisition analyses are based on platform-centric warfare (PCW) whereas the FCS will take advantage of improved communication and computing powers to shift to network-centric warfare (NCW)[1].

The tank-based force we have fielded since World War II essentially characterizes PCW. In PCW, the focus for fire and maneuver, as well as any analysis effort, is on the individual platforms, e.g. the tanks, howitzers and infantry carriers. The capability of the force is directly related to the sum of the organic capabilities of the individual platforms in that force. In NCW, the focus is away from the platforms as on the interactions between the platforms. Through

[1] We do not intend to focus this report on an in-depth description of NCW. Rather, we refer the reader to detailed discussions of this in Alberts, et al (2000) and the Naval Studies Board (2000).

increased computing and communications capabilities, the individual platforms can interact collaborate to the point that the capability of the force is much more than the sum of the organic capabilities of the individual platforms. This collaborative capability is essence of NCW and is what differentiates it from PCW.

The common expectation of this transformed force is that will derive its dominance over potential rivals by taking full advantage of a potential Revolution in Military Affairs (RMA) anchored in a host of current and near-future technological advances. The purpose of this technical report is to focus the analysis effort on that which will provide the tremendous leap in capability sought by the Army Chief of Staff. Our approach is to first establish the framework within which such a revolution occurs, based on a consensus definition of a RMA. We then exploit this definition to provide a focus for analysis.

1.1. The Framework of a Revolution

The challenge for this transformation effort is not only in the size and scope of the initiative but also history. No military has ever transformed itself following a dramatic and overwhelming victory, in this case, Operations Desert Storm and never in American Military history have we ever transformed ourselves during peacetime. On the contrary, normally we shun transformation efforts during peacetime, only to dramatically embrace them during actual conflict (Shinseki, 1999). The intervening years between the World Wars provides us with an antidotal illustration.

In the mid 1930s, military leaders like Eisenhower and Patton were promoting the potential of tank warfare. However, in spite of their efforts at swaying more senior military leaders of these potentials, their recommendations were dismissed out of hand. The rationale

was the success of American forces in World War I and the lack of a perceived threat. Eisenhower, an infantry officer, was even threatened with court martial if he persisted in his campaign of promoting tank warfare! (Eisenhower, 1967) It was the German Army that felt the need to take advantage of the potential found in tank warfare, partially as a result of their defeat in World War I. Their *Blitzkrieg* operations proved so successful and dominating that Germany nearly controlled all of Europe before the Allies were able to regroup.

The German Army developed this revolutionary tactic through the application of technology and doctrine. They did not seek to initiate a Revolution in Military Affairs (RMA), but rather developed this type of warfare out of necessity. As a matter of fact, the term RMA had not even been introduced into the military mindset at that time. Indeed, not until the seminal work in this area by Michael Roberts in 1955 was the study and identification of these revolutionary changes in warfare even an academic pursuit (Arquilla, 1997). According to most military historians, there have been a number of RMAs throughout history (Murray, 1997). In the next section, we outline some of the RMAs and contrast them with improvements in warfare that are evolutionary, rather than revolutionary, in nature to highlight the significant difference.

The origin of the current RMA debate is normally traced back to Soviet researchers in the 1970s, led by Field Marshal N. V. Ogarkov, the Chief of the Soviet General Staff. They initially termed the application of information technology to warfare as a Military Technical Revolution (MTR) and then, in the early 1990s, called an RMA. The rationale for seeking and taking advantage of a potential RMA is simple. If you do so, you have the advantage over your opponent and if you do not, your opponent will have the advantage over you. The difficulty lies

in discovering the potential revolutionary advantage prior to your opponent and leveraging its benefits.

There have been hundreds, and perhaps thousands of articles, monographs and speeches given on the subject of the "coming RMA" and its potential impact on militaries and acquisition strategies. Most of these have either debated the likelihood of this RMA or discussed broad strategic statements as to what will comprise this RMA. The latter mostly base their discussions on the four tenants put forth in *Joint Vision 2010* as to what will comprise the RMA, namely, precision strike, decisive engagement, focused logistics and full dimensional protection. These four areas provide a framework for military transformation, but they are not however sufficiently focused to develop a structure for evaluating the potential of a conceptual FCS design to provide the means of achieving the revolution we seek in the Objective Force concept.

One difficulty the Army faces in our current Objective Force endeavor is that most, if not all, previous RMAs are identified *post facto*. That is to say, the revolutionary change is normally a discussion for military historians only after its effects are displayed in actual warfare. The United States Army is attempting to define, and develop, an RMA prior to its appearance in warfare. Some claim that emerging information technology will allow us to destroy targets at a great distance using conventional, precision means. Is this the RMA? Most agree that it is more than a simple application of technology. Indeed, John T. Correll, the Editor-in-Chief of Air Force Magazine states, Technology alone does not revolutionize the way wars are fought." (Correl, 1995) The first step, it seems then, to achieving an RMA is to define what constitutes an RMA in the first place.

The Office of Net Assessment in the Department of Defense headed by Andrew Marshall has stated that a RMA occurs when technological change makes possible the introduction of new materiel that when combined with organizational and operational change, results in fundamental change in the conduct of warfare. What is important is not the speed with which a revolution takes place, but rather the magnitude of the change itself (Welsh, 1995). Others have stated that the change does not necessarily require technological innovations, but must include the organizational and operational changes.

We assert that a RMA can only occur in an environment where three preconditions are satisfied. First, there must be a fundamental change in the nature of warfare, usually, but not necessarily, through the application of technological advances. Second, there must be associated doctrinal innovation that employs these advances in novel and significant ways. Third, there must be organizational acceptance of the combination of both the technology and the doctrinal innovations[2]. We can now use this definition to distinguish between changes that are categorized as *revolutionary* and those changes that are merely *evolutionary*, which we do below.

1.2. Historical Revolutions in Military Affairs (RMA)

Below are three examples of widely recognized historical RMAs. We use these quickly to highlight the application of the definition and not to delve deeply into the historical nature of the changes.

[2] We base this definition on a synthesis from Marshall (1995), Welch (1995) and Fitzsimmons and van Tol (1994), all from the Office of Net Assessment in the Office of the Secretary of the Army.

1.2.1. The Infantry Revolution

Minor improvements in existing technology coupled with return to a classical military formation defeated the dominant military system in Europe and resulted in the end of medieval society. At the beginning of the 14th century, heavily armored knights mounted on horseback still ruled the battlefield and their feudal system controlled the land. Massed firepower of the Welsh longbow broke mounted attacks with increasing frequency over time. When combined with pike-wielding infantry in a dense, defensive phalanx, these methods could defeat the best-trained and most chivalrous knights. By the end of the century, kings had effectively used this system to advance the power of their central government to levels unseen 500 years, battles were becoming increasing bloody, and the military service of the common man gave them an increasing say in government (Rogers, 1995).

1.2.2. The Gunpowder Revolution

One of the better-known RMAs is often called *the* Military Revolution given its impact on world history. Gunpowder had existed for centuries, notably in Chinese fireworks. Once Europeans effectively harnessed this technology to artillery in the 15th century, it sparked a cycle of adaptation and improvement in firepower and fortifications in Europe. This cycle further increased the power of central governments, leading to the rise of the nation state. More powerful central governments now had the capability to finance and deploy fleets of artillery-equipped ships on expeditions around the globe. The development of gunpowder infantry weapons, along with doctrinal innovations, produced the massed, volley-firing, formation that could defeat any non-European opponent in the world. The end result of this revolution was no less than the total domination of the world by European colonial powers (Parker, 1998)

1.2.3. The French Revolution

When the cry of "*Egalite, Liberte and Fraternite*" was no longer sufficient to sustain the French Revolution against its enemies, revolutionary leaders, such as Lazare Carnot, harnessed French society to the war effort through the *levee en masse.* This act, passed in 1793, improved the French war program by conscripting soldiers for the armies and mobilizing the civilian population for increased production of weapons and supplies. There was really no inherent technological change in this period, but the organizational acceptance guaranteed by the *levee*'s prescriptions permitted the full exploitation of pre-existing technological and doctrinal innovations to defend the Revolution. It was in this environment that Napoleon Bonaparte, possibly the greatest general of all time, had his start. It was this decree that allowed him to wage war successfully against every other power for twenty years, disrupt the existing European political system, and reorder much of the continent (Rothenberg, 1978).

1.3. Evolutionary Changes in Military Affairs

The discussion of evolutionary changes in military affairs is as controversial as identifying RMAs. An evolutionary change does not mean that the change, or the technology, is not significant. On the contrary, many evolutionary changes provide vast leaps in capabilities. The difference that we highlight here is that these increased capabilities are improvements in the conduct of warfare, and do not provide a fundamental change in the nature of warfare. Two quick examples follow.

1.3.1. The Machine Gun

In the last half of the 19th century, inventors and ordnance experts experimented with ways to increase the rate of fire for infantry weapons. These projects included the Gatling gun, magazine-fed rifles, and a number of gas-powered automatic weapons collectively known as

machine guns. Although this technology had attained a high degree of technological maturity, leading military organizations refused to fully accept its defensive potential for the battlefield in the first decade of the twentieth century. The continued myopic reliance on the individual rifleman was a key contributor to the development of the stalemate on the Western Front from 1914-1918 and the slaughter that followed. The machine gun did not change warfare, but it certainly ended face-to-face battles between masses of infantry (Ellis, 1975).

1.3.2. The Aircraft Carrier

The marriage of aviation technology to naval doctrine first occurred in the years before World War I. However, in a world dominated by the battleship and the theories of Alfred T. Mahan, the acceptance of the new weapon system was slow in coming. Naval treaties did not address carriers and many in the U.S. Navy still preferred the battleship. The Battle of the Coral Sea between the U.S and Japan in May 1942 was the first naval battle in history in which the main combatant ships never saw one another. The example provided by the projection of aircraft from a carrier vessel made the battleship relatively obsolete and changed the way fleets fought but did not noticeable alter the role of navies in warfare (Hoyt, 1989).

1.4. Summary

Some theorists, including Michael O'Hanlon from the Brookings Institution, do not agree that we will achieve a true RMA through information technological innovation. They claim that technological advances required for vastly increased capabilities to pinpoint enemy positions will not be realized at any time, let alone in the near future (O'Hanlon, 2000). We do not, in this report, enter into the fray over the pace of technological innovation *per se*. Even those most ardent doubters of the pace of technological advance acknowledge the potential of distributed

information warfare, or network-centric warfare. We do assert that by focusing our research and development efforts, we can attain the most crucial technological advances. We propose such a focus in this report.

In this introductory section, we have established a framework about which to focus our efforts, namely the preconditions for a RMA. In sections 2 and 3, we discuss the fundamental change in the nature of warfare gained through NCW and the capabilities required to leverage this change. Similarly, in sections 4 and 5, we discuss the final two preconditions, required doctrinal changes and organizational acceptance, respectively. We now turn our discussion to the engagement process and the changes that occur therein through the shift from platforms to networks.

2. Fundamental Change in Warfare

We begin our identification of the fundamental change in warfare enabled by technology in NCW by first realizing that which will not change in future warfare.[3] From the collection of essays by Major General Scales, then the Commandant of the United States Army War College, we learn, among other things, that the nine principles of war will not change (Scales, 1999). Though these principles were introduced by Jomini in the 19th Century and formalized in 1949, they will continue to form the basis for successful operations in all foreseeable future warfare. Therefore, looking to these principles as a framework for an RMA will not yield the fundamental change we seek.

The ability to mass fires, or effects, will be significantly enhanced through NCW. Whereas this is often touted as a revolutionary achievement, the process for this remains the same as the concepts in the AirLand Battle Doctrine developed in the early 1980's. As it still retains a similar process, this change is evolutionary, and not revolutionary.

There will undoubtedly be significant improvements in battle management gained through increased situational awareness. The result may be an elimination of the written field order, which will be replaced by pure graphical representations of orders sent throughout the battlespace. This alone will allow a dramatic rise in the tempo of the battle, but does not change the hierarchical nature of the basic orders process. Hence, this is an evolutionary change and is not where we will find a fundamental change that we can exploit for an RMA.

---

[3] The US Army Training and Doctrine Command (TRADOC) asserts that there is no change in the *nature* of warfare but rather a change in the *conduct* of warfare. In this report, we use the term *nature of warfare* for congruence with previous descriptions by the Office of Net Assessment, directed by Andrew Marshall. We believe our use of the term is in keeping with the intent of the distinction made by TRADOC.

Similarly, the decision to shift from a 70-ton main battle tank-equipped force to a 20-ton (or so) vehicle-equipped force improves the deployability of the force. Getting a unit to the fight quicker is certainly a necessary step for future conflicts. It is important to note, though, that the basic deployment process does not change. We still transport units via air or ground to get to the battles. We can now get them there quicker and closer so to better influence the battle, but as the process does not change, we will not gain the RMA in this area.

Furthermore, the reduced size of the vehicle types has an impact on the logistics of the force. Smaller, more efficient vehicles result in a change in the reliance of the force on resupply. Though we can reduce the resupply burden of the force through evolutionary improvements in engine efficiency and water retention, the necessity for periodic resupply by current means remains. Hence, there is not a fundamental change in the resupply process.

The above commentary on the potential improvements with the FCS-equipped force in massing fires, battle management, deployability, and logistics is not intended to trivialize the significance of these areas or to direct attention away from them. These remain significant innovations that are absolutely necessary to keep the force dominant throughout the spectrum of warfare. Our intent here is to simply focus the discussion on the part of the FCS-equipped force that will provide us with the fundamental change we seek for an RMA. We discovered this by focusing on the shift from platforms to networks.

The basic change between platform-centric warfare to network-centric warfare removes the focus on platforms. Therefore, the combat processes performed at the platform level drew our scrutiny and yielded the fundamental change we were seeking. The basic procedure for engaging enemy targets changes from a wholly organic process in PCW to a collaborative,

distributed process in NCW. Upon further analysis, we determined there are five distinct information functions to complete the process. We term these five functions as the **Battlefield Information Functions**, or BIF, and they are Search/Detect, Identify, Target/Track, Engage and Assess. These BIF become the framework for our analysis of the critical aspects of the FCS conceptual design alternatives. Essentially, accomplishing these BIF seamlessly, collaboratively and distributively, will achieve the fundamental change in the nature of warfare; the first precondition for a RMA. We continue below with a more in-depth look at how this process changes in information warfare.

2.1. Process Changes

Figure 1 below, depicts the five BIF in PCW. As shown, this is a sequence of five distinct steps an individual, or a crew, follows to engage the enemy. Only after completing the process can the individual, or crew, restart the procedure for each subsequent engagement[4]. In a platform-centric force, reducing the time to complete the process, or to restart the process after completion, increases the probability that you kill the enemy before he kills you. Hence, this reduction in process time has always been a paramount objective in military research and was therefore, one of the objectives in the digitization effort associated with the Force XXI initiative.

For a direct fire engagement, the individual or platform crew conducts these steps sequentially and individually. In other words, each step in the engagement process is conducted *organically*. For an indirect fire engagement, there is only a change in the "Engage" step in the process. This is the case for calls for artillery and even for Hellfire missile engagements using the OH-58D lasing system in conjunction with the Apache. All other steps are done organically

and the engage step is initiated via request from the platform directing the other steps in the process. In other words, it is not automatically directed and the steps are conducted by the same system.[5]

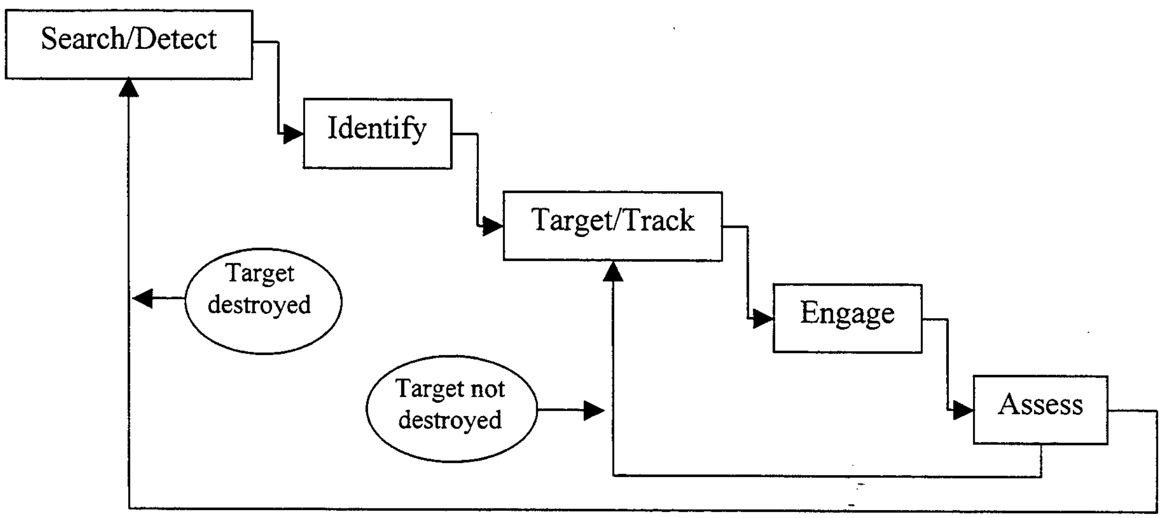


Figure 1: Engagement Process in Platform-centric Warfare[6].

Through the digitization of the individual platforms, the Force XXI initiative successfully reduced the process time by improved situational awareness, targeting and identification of friendly forces. Though this was a great enhancement, the process itself was not changed. Thus, the change in warfare due to digitization was *evolutionary*. Individuals, or the individual crews,

---

[4] This process is changed slightly for the M1A2 in that the Gunner's station and the Commander's station are unslaved allowing the Commander to identify while the gunner engages.

[5] The exception would be engagements direct by the Q36 counter fire radar. Though these engagements are computerized, the assessment process is by exception in that we assume destruction when the enemy stops firing.

[6] This process was extrapolated from the description found in Department of the Army Field Manual 17-12-1-1, "Tank Gunnery (Abrams) Volume I – Tank Crew Handbook", Washington, DC, 5 May 1998, with the exception of the feedback loop. This is also a modification of the functional flow process described in Development and Readiness Command (DARCOM) Pamphlet, 706-101, "Engineering Design Handbook – Weapon Systems Analysis, Part One", Department of the Army, November 1977, p 11-9.

in the Force XXI platform-centric force still conducted each step themselves. NCW fundamentally changes this dynamic.

In NCW, each step in the engagement process can be conducted by elements other than the individual, or the individual crew of the platform. All steps can now be conducted *collaboratively*. That is, different agents conduct the steps in the process at the same time across the battlefield and are linked to each other via a computer communications network. This allows parallel processing through the engagement cycle as depicted in Figure 2. While some assets within the battlespace are searching and detecting entities, others are identifying, still others are targeting and tracking. Engagements and assessments can be accomplished at the same time by distributing the capabilities throughout a force.

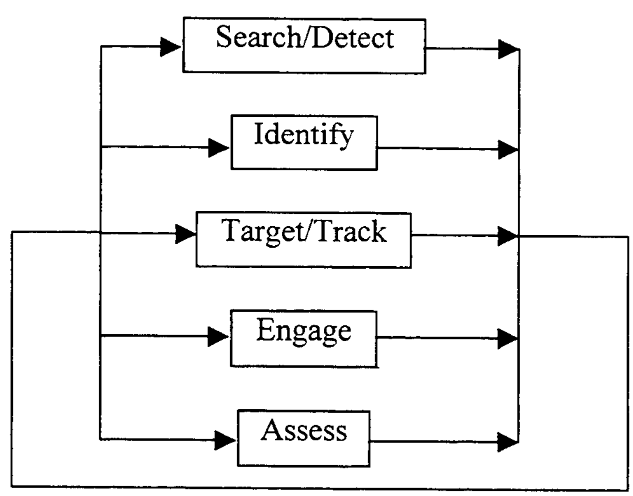


Figure 2: Engagement Process in Network-centric Warfare

This parallel processing fundamentally changes the dynamics of the engagement process by changing the nature of time as a driver in Decision Making/Combat Operations within engagements and between subsequent engagements. This is only now possible due to the capability to synthesize information by distributing sensors and computing power throughout the

battlefield. It is this “distributed nature” of Information Warfare (IW) in a network-centric force that supports, or arguably allows, for the first time continuous, parallel operations in all five modules of the process. This represents a *revolutionary* advance in the very structure of warfare.

A digitization goal was to link a sensor to a shooter. In NCW, we can use distributed computing power to link many sensors to many shooters. These multiple sensors work collaboratively in a seamless distributed network to provide information to multiple shooter platforms throughout the battlespace. Distributed computing power will allow the information gained by distributed sensors to be passed to multiple shooters for the engagement. In other words, we no longer have to rely on organic capabilities to follow the sequential steps of the engagement process. We now can do so collaboratively. In section 3, we expound on the specific capabilities required in a system to allow the system to operate effectively using this collaborative capability. We continue here with a comparison of PCW and NCW capabilities.

The engagement process for a platform-centric force in a battle is depicted in figure 3, below. In this “battle”, there are four separate platforms. Each platform sequentially follows the steps in the engagement process for each of the enemy targets (shown as triangles in the figure). Once should note that for each enemy target engaged, the entire process is conducted using only organic assets and that the process must be restarted and completed for each separate “engagement”.

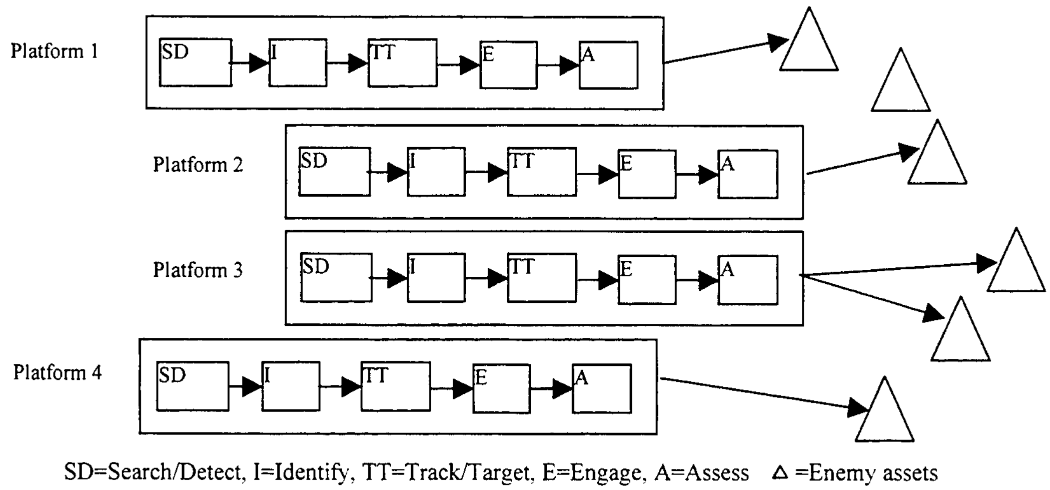
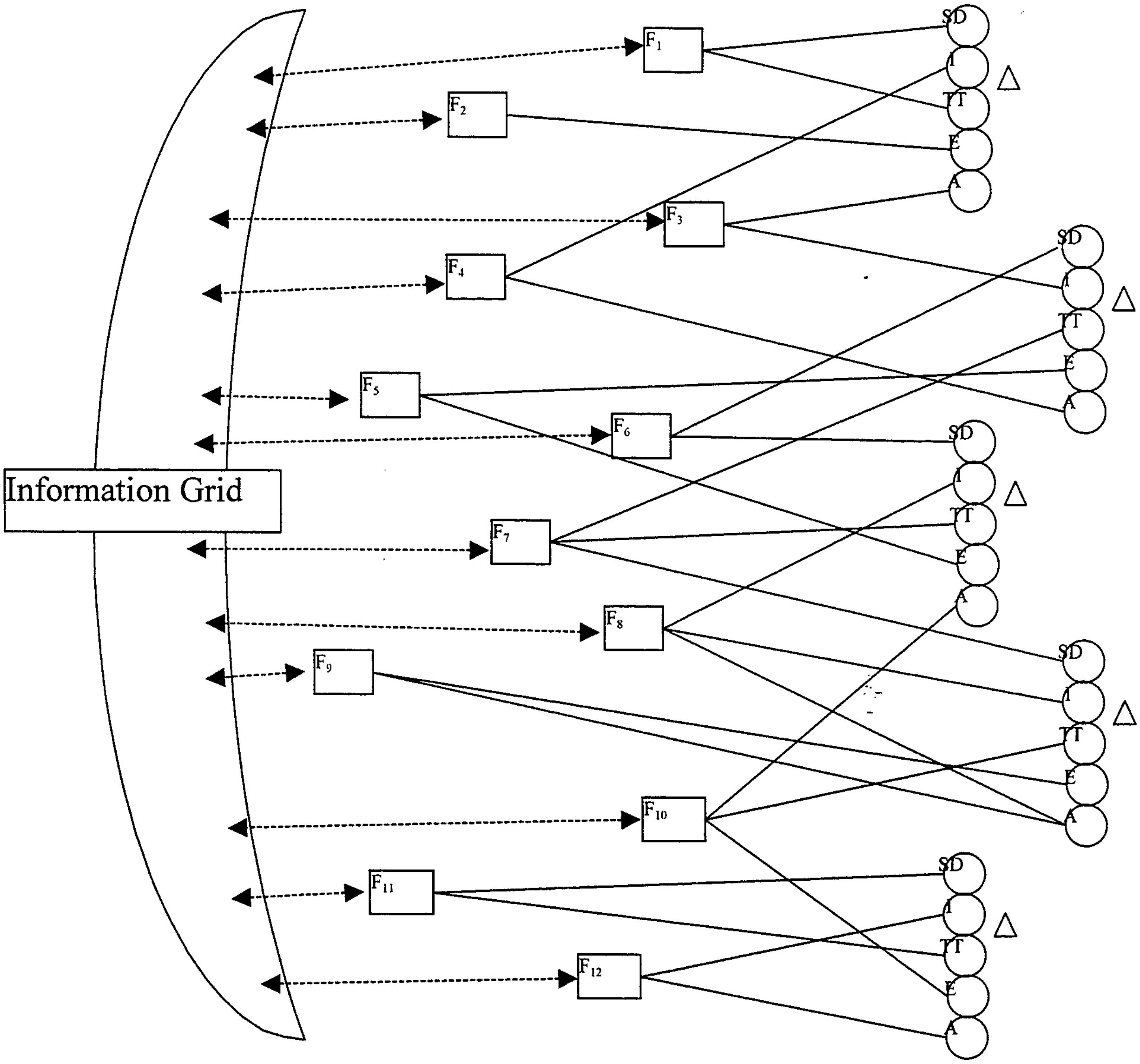


Figure 3: Platform-centric force engagement architecture

Contrast this to essentially the same "battle" for a network-centric force, as shown in Figure 4, below. As this figure shows, from the perspective of the enemy (shown as triangles), the "steps" are still followed logically and sequentially, but not necessarily by the same friendly entity (shown as squares). In this figure, the solid lines from the Friendly entities link that entity to the function performed *on* the enemy entity and for all friendly entities in the battlespace. The information gained by the friendly entities performing a function is passed to all entities through the information grid. This figure depicts a peer-server relationship, however, a peer-peer relationship would be more consistent with the NCW requirements.



SD=Search/Detect, I=Identify, TT=Track/Target, E=Engage, A=Assess   Δ=Enemy assets   □=Friendly entities

Figure 4: Network-centric force engagement architecture

This sharing of information and capabilities between platforms creates an interdependence, which replaces the independence of the platform-centric force. From the friendly perspective, the BIF are no longer "steps" as conceptually time and sequence are removed from the process. The distributed nature of information warfare shifts the focus from organic capabilities to collaborative capabilities. We continue with an example to highlight the

specific aspects of organic and collaborative capabilities and then describe the Navy's application - the Collaborative Engagement Capability (CEC).

2.2. Organic System Capabilities

In a platform-centric force, that platform's organic assets accomplish each step in the engagement process sequentially and must start the process anew for each engagement. The digitization effort in the Force XXI initiative greatly improved the early warning capabilities in the system and the prior identification. Additionally, recognition capabilities designed into the digitization effort, especially the ability to track friendly forces, greatly improved the ability to properly identify friend or foe. These advancements allowed an M1A1 Abrams tank crew, for example, to greatly reduce the time required to complete the cycle and defeat the enemy.

The following is an excerpt from an interview of Lieutenant Colonel (then-Captain) H. R. McMaster, Jr., conducted by Tom Clancy in his book *Armored Cav*. LTC McMaster was the Cavalry Troop Commander of the lead unit in the tank battle known as *The Battle of 73 Eastings*. This was the most notable tank battle since World War II and epitomized the equipment and leadership dominance US forces enjoyed over the Iraqi forces. In this excerpt, LTC McMaster describes when his armored cavalry unit, Eagle Troop, first encountered and then engaged the Iraqi Tawakalna Division of the Republican Guard.

> ...As Staff Sergeant Magee's gunner, Sergeant Moody, engaged the T-72, my tank crested an almost imperceptible rise in the terrain. I immediately spotted eight enemy tanks in a defensive position oriented west (in our direction). The sandstorm had died down, and visibility had improved enough to see them with the naked eye...I reported "contact" to the troop and...[a]t the same time, I gave my crew the command to fire, and my gunner Staff Sergeant Craig Koch, destroyed three of the enemy tanks in under ten seconds...I thought at the time that they were T-55 tanks because we were destroying them so quickly. The enemy return first was also ineffective. Several T-72 tank rounds fell short and their machine-gun fire had no effect on the armored vehicles....[Eagle Troop

> destroyed] approximately thirty tanks, sixteen BMP infantry fighting vehicles and thirty-nine trucks. The outcome of the battle I am most grateful for, however, is that Eagle Troop suffered no casualties. I thank God for that (Clancy, 1993).

There is no questioning the effectiveness of this force nor is there any dispute as to its complete dominance of the battlefield. Though LTC McMaster's tank was able to destroy a number of vehicles (including "three of the enemy tanks in under ten seconds") the capabilities of his tank were due solely to the organic assets on that tank. This is highlighted by an analysis of the engagement process LTC McMaster followed.

After cresting "an almost imperceptible rise in the terrain", LTC McMaster's tank visually detected tanks. This is the Search/Detect step in the process. Notice that although LTC McMaster, via radio, may have been alerted of potential enemy tanks in the area and even given a grid positioning to find the tanks, it was only when he detected the tank with his organic assets that they began the engagement process on this enemy.

The identification of these enemy tanks was relatively straightforward. LTC McMaster's unit was in a firefight with other tanks. These were identified as enemy tanks by their location as well as their distinctive features as they could be seen "with the naked eye". As these tanks that he visually detected were near the other enemy tanks, he could assume with reasonable certainty that they were indeed enemy tanks. This is not always the case as is borne out through counter examples of friendly fire incidents in Desert Storm.

LTC McMaster's gunner, SSG Koch, conducted the targeting/tracking and the engagement steps so quickly that the difference between the steps was almost imperceptible - an obviously well trained gunner. Regardless, this well-trained gunner conducted both of these steps prior to moving on to the next enemy tank.

LTC McMaster himself conducted the final step in the process, the assessment. Only after seeing the tanks destroyed and determining the return fire had stopped could the battle be assessed as completed and the enemy destroyed. Again, this was done with organic assets requiring direct contact with the enemy.

We do not contend that the presence and actions of the rest of the troop did not effect the outcome of the battle. On the contrary, each member of the troop, and squadron, played their role in this victory. We merely use this as a vignette to support our contention that platform-centric warfare relies upon the organic capabilities of each individual platform. Had the enemy been better trained, in more compartmentalized terrain or had better equipment, LTC McMaster may not have been able to boast that "Eagle Troop suffered no casualties" from this direct contact with the enemy. NCW and collaboration will not completely eliminate the necessity to close with and destroy the enemy. It would have allowed this complete destruction of the enemy from out of harm's way by engaging collaboratively from greater distances. In this next section, we will describe how the collaborative system capabilities fundamentally change the engagement process in a network-centric force.

2.3. Collaborative System Capabilities

We do not, in this section, attempt to quantify or assess the technology available in any given timeframe. We intend to present the previous vignette described by LTC McMaster in a network-centric warfare context to highlight the collaborative nature of distributed information warfare.

In a scenario such as the one LTC McMaster's troop found itself, a network-centric equivalent force would not have been that close to the enemy, in all likelihood. After "spotting"

the enemy with the aerial sensors from either the Air Force assets, assets from an adjacent unit, or even the unit's own sensor assets, every friendly asset in the area would have immediately (or nearly so) determined the location and composition of the enemy tanks and other vehicles. The sensor assets from all localized units can target each of the detected enemy vehicles simultaneously. The targets are then engaged, with varying munitions depending on the target vehicle type, and from varying locations depending on the threat surrounding the firing unit. Hence, the firing unit does not even have to sense the enemy with its own sensors, nor do they have to have to track the enemy or the missile with organic assets.

Note here that as opposed to the platform-centric force, many varied, distributed friendly assets perform the functions of detecting, identifying, targeting, engaging and assessing simultaneously. No longer is an asset forced to rely on its own organic capabilities to destroy the enemy before the enemy destroys him. This is much more than friendly assets sharing their organic capabilities. This is about integrating specialized organic capabilities of dispersed assets in such a manner as to optimize the effectiveness of the overall unit as opposed to the individual platform.

It is through the distributed nature of warfare that this collaboration of systems is possible. Just as each system supports the actions of other systems in the battlespace, each system relies on the others for realization of its capabilities. For example, a sensor has no capabilities if there is nothing to act on that sensor's discoveries. Similarly, an effective sensor can provide searching, detecting, identifying and tracking information to an effective "engager" making the overall systems capabilities greater than the sum of the individual sub-systems themselves.

The effectiveness of the distributed nature of information warfare is not notional, nor is it science fiction. It has been demonstrated very effectively in the Navy in their Cooperative Engagement Capability (CEC) as part of the Aegis battleship found within Carrier Battle Groups. (CBGs). In this next section, we describe this CEC and its effectiveness. While the tasks and conditions faced in the Army are very different from most Naval engagements, this provides an illustrative example of the potentials of leveraging this capability.

2.4. Cooperative Engagement Capability (CEC)

The Navy's Cooperative Engagement Capability (CEC), developed jointly with the Applied Physics Laboratory (APL), demonstrates the tactical and operational impact this collaborative capability and the distributed nature of IW has. This system of networked sensors and shooters has been successfully demonstrated as a defense system against incoming ballistic missiles as well as serving as a power projection platform for Naval effect on shore.

Admittedly, conditions are different for Naval operations as opposed to Army operations. These differences are mostly technological challenges vice operational requirements. For example, the Navy operates in an environment where communications are relatively obstacle free. The Army must overcome the effects of terrain among other things as part of their communications challenge. This does not obviate the need to use the Naval approach for insights into the capabilities required in the Army's exploitation of network-centric warfare. The requirements are very similar, as gleaned from the passage below from APL:

> Coalescing this collection of equipment into a single war-fighting entity requires a system that will [share] sensor, decision, and engagement data among combatant units, yet without compromising the timeliness, volume, and accuracy of the data. The system must create an identical picture at each unit of sufficient quality to be treated as local data for engagements, even though the data may have arrived from 30 to 40 mi. away. If a common, detailed

database is available to provide a shared air picture as well as the ability to engage targets that may not be seen locally, a new level of capability may be attained (See "Cooperative Engagement Capabilities", 1995).

The CEC is a proven and fielded system of systems aboard most Aegis cruisers and some Carrier Battle Groups (CBG). This system collects data from sensors, both new and legacy systems, and integrates that information into a common picture for each of the individual assets within a battle group. In this way, the picture that each receives reflects the information in a useful manner for that asset. In other words, an asset within the battle group (be it a sea-based ship or a land-based Marine unit) can obtain information on enemy, friendly and non-combatant movements at their location even though their sensors may not be sensing the action themselves. This capability is even more strikingly significant for engagements.

During an engagement, a system may fire a round that eventually destroys the target though its organic sensors and radars never pick up either the target or the round but rather sensors elsewhere in the battle space conduct the target identification, precision targeting and the round tracking required for intercept, destruction and assessment. These sensors could be airborne, ground-based, sea-based, and even elements of another service (e.g. Patriot) or Allied Force. Additionally, by distributing the information and the sensor/tracking requirements, disabling one, or even many, sensors/radars would not diminish the capabilities of the entire system, so long as there is one, distributed, linked sensor/radar yet available in the battle space.

The distributed nature of IW improves the capability of the individual systems by providing increased accuracy in targeting through the synthesis of information from many sensors. It provides increased survivability of the sensor network by distributing the computing requirements throughout the battlefield so that even if one system is destroyed, there are others

that can accomplish the same tasks. The CEC deployed by the Navy demonstrates the usefulness of the collaborative capabilities of systems that are automated and connected by networks. The question that remains, however, is "how do we know that this collaborative, distributed capability is actually better than merely technologically advancing our current platform-centric forces?" In the next section, we turn to mathematics to answer that question.

2.5. Global and Local Optimal Strategies

As it is difficult to imagine a new type of force, it is also difficult to explain how this force could be better than our current method of operations. To this end, we turn to a basic principle of mathematics, that of global and local optimization. Optimization is the science of choosing the best option from a feasible set of alternatives given a set of constraints. Global optimization is the best solution over the entire set of feasible solutions. Local optimization is a best solution within a range of feasible solutions. In a pure attrition-based combat situation, optimization may take the form of determining the best combination of firing platforms, munitions and orders of firing to completely destroy the enemy target set. For the purposes of this discussion, we will use that as our conditions for analysis. A closed form direct formulation of a problem as complex as combat is virtually impossible, therefore, we look at this problem from a theoretical standpoint.

In a platform-centric force, combat provides a series of engagement decisions made by each individual platform. Without the benefit of collaboration, these decisions are "solved" locally by each platform using its own organic capabilities in an attempt to maximize its successful engagements based on its own set of constraints and objective criteria. In this way, each individual platform determines its own *locally* optimal solution to the problem. In this

manner, the effectiveness of the overall force is some functional form of the collection of each of these individually, or locally, optimal decisions. Analytically, this is represented as follows for *n* separate platforms:[7]

$$OPT\ f_i(SD, I, TT, E, A),\ for\ i = 1 \ldots n \qquad (2.1)$$

and the effectiveness of the overall force is represented as follows:

$$Z_{pcw} = f(OPT\ f_i(SD, I, TT, E, A),\ for\ i = 1 \ldots n) \qquad (2.2)$$

with Z_{pcw} being the overall effectiveness of a platform-centric force.

Now, we compare this to a network-centric force. In this force, the information is processed and distributed to all friendly entities in the battlespace. The engagement process is managed collaboratively. This way all decisions are optimized throughout the battlespace, or across the range of the constraint set. Thus we have only one optimization, which then provides us with a globally optimal solution. The mathematical representation of this is:

$$Z_{ncw} = f(OPT\ f(SD_i, I_i, TT_i, E_i, A_i),\ for\ i = 1 \ldots n) \qquad (2.3)$$

It is a well established fact in mathematics, whose proof we do not detail here for practicality, that a globally optimal solution is never worse than some functional summation of numerous local optimal solutions.[8] With this in mind, we view Z_{pcw} as a combination of local optimal solutions and Z_{ncw} is a global optimal solution. As such, we can be assured that Z_{ncw} will always be at least as good as Z_{pcw}, and will, in most cases, be better. This mathematical vignette provides sufficient insight and proof that the capabilities of NCW will exceed the

[7] Note that the actual functional form of this relationship is not germane to the discussion.

[8] We do not discuss the proof behind the superiority of a global optimal solution over a local optimal solution here. For a formal proof, the reader is referred to Bazaraa, et al (1993), pp. 99-101, among others.

capabilities of PCW, assuming that the correct capabilities of NCW are identified, developed and integrated. That is the purpose of this report.

It is intuitive that given information about the overall situation, a commander, or even a shooter, can make better decisions. The major difference between the PCW and the NCW is that in NCW these decisions are made using information from the entire battlespace whereas in PCW, these decisions are made using information from solely organic assets available to the individual platform.[9] Using collaborative capabilities found through network-centric warfare enables a commander to optimize his or her assets in the entire battlespace, immediately. This is clearly a better method of fire control, both intuitively and mathematically.

2.6. Summary and Directions

In this section, we have identified the very kernel of the potential Revolution in Military Affairs afforded by technology. This fundamental change in warfare is found in the Engagement Process and the five Battlefield Information Functions (BIF) that make up this process. As this is the kernel of the RMA, focusing our analysis of the FCS conceptual design alternatives on these BIF will ensure the fielded systems can accomplish the potentials sought in the RMA. In section 3, which follows, we recommend a means to do just that. These BIF should also be the focal point for the Army's research and development efforts. Failing to develop the proper technology within the given timeframe to enable this collaborative, distributed engagement process, runs the

---

[9] We concede that there are opportunities for fire control within a force during an engagement using voice commands. Here we are considering the automatic processing capabilities of a network-centric force. Given the immediacy of information required in making truly globally optimal solutions regarding engagements, the use of these representations are justified.

risk of attempting to field a system with only moderately improved capabilities over the existing force. This could jeopardize funding for future iterations of the FCS.

3. Battlefield Information Functions (BIF)

In this section, we delve into the details behind the Battlefield Information Functions (BIF) introduced in the previous section. These five functions form the framework about which we will focus our analysis of the conceptual design alternatives for the Future Combat System (FCS). We present this discussion in three main sub-sections: Distributed Information Warfare, Collaborative Information Requirements, and Future Combat System Requirements.

In the first sub-section, Distributed Information Warfare, we discuss the changing nature of each BIF realized through the application of distributed information warfare. This is a more detailed discussion of the capabilities addressed in the previous section.

In the second sub-section, Collaborative Information Requirements, we discuss the information for the FCS as part of a larger Objective Force capability. We recognize that the FCS will operate in tandem with other forces on the battlefield. These forces will be part of the Objective Force, other FCS units, Joint assets and possibly even allied forces. To facilitate this discussion of information requirements, we introduce the term Objective Force Information Grid (OFIG). Each BIF requires specific information inputs to the OFIG and information requirements from the OFIG to effect collaborative engagements.

In the third and final section, Future Combat System Requirements, we focus on the organic capabilities of the FCS. Here again use the BIF as our framework. We identify individual capabilities of the system to provide information requirements identified in the previous sub-section and operate as an organic system of systems. We also identify key metrics used to evaluate the operational success of the FCS.

3.1. Distributed Information Warfare

3.1.1. Search/Detect

The entire Engagement Process begins with searching the battlespace and detecting entities, potential adversaries, friendly forces and non-combatants. As it is the start of the process, it sets the stage for all other modules and the success of all the other modules rely on its performance.

The distributed nature of information-based NCW changes the dynamics of the search/detect function of the engagement process more than of the other four functions. Even with the application of digitization in the Force XXI Army, a tank commander still relied on his own organic assets to scan and detect entities within his Area of Operations (AO). Sensors could identify movement, scouts could warn of impending danger in the form of on-coming enemy forces, and visual aids such as the introduction of improved optics and night-capable systems (such as Forward-Looking Infrared (FLIR) systems) increased capabilities, but generally, real-time searching and detecting targets remained the responsibility of on-board, organic systems. Distributing the searching and detecting requirements and the distributed coalescing of the information for a local common picture fundamentally changes not only the capabilities in this module, but also the module itself.

In this search/detect function, we do not limit our analysis to the capabilities of sensors alone. In distributed Information Warfare, our capabilities to search and detect will come from many sources. Hence, we expand our focus to account for all Information Operation (IO) assets in the battlespace. IO assets from one system provide information to all other systems in the battlespace. Similarly, every command asset in the battlespace has access to the information obtained from IO assets throughout that battlespace. This information needs to be seamlessly

coalesced to provide every command asset with a common picture of their area of concern, and can be modified based on movement of the unit or changes in missions.

The benefits from the distribution of this function are many. By distributing the search/detect requirements, the power of the information from the IO assets increases exponentially. The information is no longer reserved for the entities to which the IO assets are organically linked. In a digitized force, the information gleaned from organic sensors was passed from lower to higher and then back down the chain to the other assets in the larger organization. The problem with this was two-fold: First, the timeliness, or currency, of the information was reduced. Second, the system relied on links in the chain to not be disrupted. In a distributed information system, information obtained from one set of IO assets can be immediately processed and transmitted to every other asset in the battlespace for their use.

Searching and detecting a warfighting entity within a battlespace is very difficult in the environment the Army will find itself, as opposed to the environment faced by the Navy or the Air Force. For the other services, the movement of and jet or a missile distinctly different than a bird, much like the movement of a submarine or a torpedo is different than a fish. For the Army units, there is great difficulty detecting a soldier or a vehicle that is not moving and is properly camouflaged. Differentiating that soldier or vehicle from a tree or a shrub is even more challenging. By distributing and linking different IO capabilities and then integrating them through knowledge management, Army forces can overcome the challenges of detecting entities brought on by their efforts of detection-avoidance.

3.1.2. Identify

With the taste of the friendly fire incidents during Operation Desert Storm and again during Operation Provide Comfort still sour in America's mouth, the Army in the early 1990s placed renewed emphasis on the ability to properly identify friendly assets. The cost of either identifying a friend as an enemy or an enemy as a friend could be equally deadly on a battlefield. When provided the capability to sense entities 200km away and then engage them at a range of over 150 km, passive identification of friend or foe is insufficient. We must be able to positively, promptly and accurately identify entities throughout the entire battlespace. Fortunately, the distributed nature information warfare in a network-centric force can greatly increase our capabilities in this vital area.

One of the drawbacks of the distributed nature of information warfare is the increased number of friendly entities in a battlespace. Whereas the platforms of the systems are more greatly dispersed, there are many more platforms and sensor assets, especially airborne sensors. Arguably, the destruction of unmanned sensor assets is clearly not as significant as the destruction of a manned platform, but it still effects the capabilities of the force and is not desirable. This dispersion of forces, however, serves to improve our abilities to identify and classify entities that have been detected by our sensors and thus outweighs the increased requirements for detecting numerous targets.

By distributing the computational requirements and sharing information in real time, we can immediately add to our inventory of friendly assets any actor that enters our battlespace. For example, when a entity departs its location all other units in the battlespace immediately recognizes that entity as friendly upon its entry into the information network. Even in the event

of decreased capabilities due to downed communication links or other mishaps, the computing assets within a unit sends the proper information upon resumption of contact.

Now let us take this example one step further. Assume an FCS-equipped unit (regardless of size) completely breaks contact with all other units within a battlespace. That FCS-equipped unit then encounters another friendly unit or sensor asset, or conversely the unit or sensor encounters them. Communications are re-established and, hence, the unit is immediately recognized as a friendly asset.

The identification process in a platform-centric force is depicted in figure 4. Here, the arrows represent the identification of friendly assets. Hence, in the platform-centric case, for Asset A to identify Asset B, C and D as friendly, each must be identified by Asset A, individually.

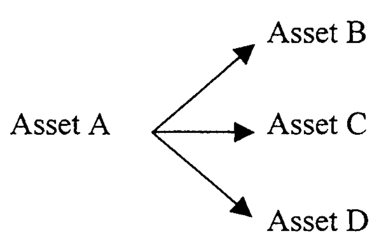


Figure 4: Friendly asset identification in a platform-centric force

Conversely, figure 5 represents the identification of these same assets in a network-centric force. Here each asset can use the identification information obtained by another asset. This reduces the individual assets information requirement by distributing the identification process.

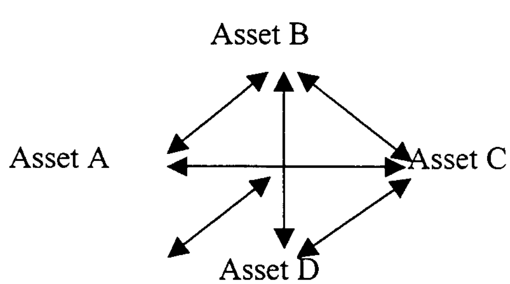


Figure 5: Friendly asset identification in a network-centric force

In this manner, distributed information warfare hastens the identification of friendly assets. This also serves to help differentiate between friendly forces and either enemy forces or non-combatants. Unfortunately, differentiating between non-combatants and enemy forces is not quite as straightforward.

3.1.3. Target/Track

Targeting and tracking the enemy, as well as tracking non-combatants as necessary, is a function well suited for distributed information warfare. As described in the CEC illustration presented earlier in this paper, two or more sensors are required to conduct precision targeting. Tracking an enemy target in a platform-centric force was limited to the range and capabilities of the individual sensor radar. In a network-centric, distributed force, any sensor in the area can track the target and provide that information for the benefit of all friendly assets in the battlespace. The target can then be passed off to any other sensor radar in the battlespace that can sense the target. The hand-off is automatic and continuous. It does not depend on the boundary lines of the individual units, nor the range or capabilities of individual sensors.

The ability to distribute sensors will greatly improve our targeting. As stated in the description of the CEC by APL (APL, 1996), targeting using two or more sensors increases the time required for "precision cuing" of assets throughout the battlespace. This means that even though a system's organic sensors do not detect a threat their engagement assets can be cued to direct firing through distributed, forward deployed sensors. This is critical in an asymmetric, non-linear battlespace as the type we anticipate being the FCS-equipped Objective Force operating environment.

3.1.4. Engage

The process culminates in this module in distributed information warfare as it does in platform-centric warfare. The difference is in the timing of our effects and the capability to integrate multiple processes at one time. This is not simple but it is required to attain the battlespace dominance required of this FCS-equipped Objective Force. Distributed information warfare improves our ability to engage the enemy through the increased ability to attack the enemy from Beyond Line of Sight (BLOS) and efficiently distribute fires automatically. Through our increased ability to sense, detect, identify, track and target the enemy and with a networked, distributed engagement capability throughout the battlespace we can now remotely engage the enemy anywhere in the battlespace. By remote engagement, we mean that we can not only fire direct fire from an unmanned system, but also fire from a system that is not organic to our own unit.

The collaborative nature of distributed information warfare is probably most clearly illustrated in this engagement module. In a platform-centric environment, the closest thing to collaborative engagement (or Cooperative Engagement Capability to use the Navy/Aegis term) is the direction of long-range artillery. For these missions, a forward observer would call for fire and wait for a unit, possibly unknown to him, to fire a round. The observer would then observe the impact, adjust, and eventually request a "fire for effect" or multiple-round engagement. This can be done immediately in a network-centric distributed force for all engagements.

After an enemy entity in the battlespace is detected, identified, tracked and targeted, any system within range can engage. Imagine an FCS-equipped unit hidden forward in a battlespace, possibly within direct fire range of some enemy assets. That unit possibly should not directly engage the enemy, as it would give away its position, even while firing from remote, unmanned

platforms within the unit. Using collaborative engagement capabilities, however, that unit can automatically direct another unit to fire at the enemy.

This collaborative capability is even more powerful in a distributed fire context. The system can automatically adjust the firing unit as it senses a given asset is low on ammunition or may receive increased threat in the near future. This eliminates the requirement to cross-load ammunition between platforms to provide proper coverage. This also reduces the logistic burden on forward-deployed units by leveraging the direct, precision engagement capability of every available firing asset in the battlespace.

3.1.5. Assess

After engaging a target, we must determine whether we must re-engage that target. Failure to re-engage a target that has not been destroyed can result in an enemy being able to destroy us. On the other hand, re-engaging a target that has already been destroyed unnecessarily burdens our logistic system. Fortunately, the distributed nature of information warfare can reduce these types of errors.

As with the other BIF, the ability to assess damage will be greatly enhanced through distributed information warfare. Previously, platforms relied on their own visual detection of damage, or possibly the voice communications from other assets on the battlefield. Distributed information warfare will not only allow sensing from various sources, but also the ability to change our definition of damage by using different types of sensors in conjunction with one another. For example, before we possibly identified a enemy entity as destroyed through the lack of movement. Now we can also combine that with thermal sensors from another source to possibly identify reduced body temperature due to death, or the combination of the other

technologies. Thus distributed information warfare not only will allow the immediate dissemination of the status of a previously engaged enemy system, but also allow us to determine if he is just "playing possum".

3.2. Collaborative Information Requirements

Within each BIF there are two general categories of information requirements to facilitate the collaborative capabilities of the overall FCS. The first category is information requirements processed between the FCS and assets external to the FCS. The second category is information requirements within the FCS. In this sub-section, we focus on the former while in the next sub-section we focus on the latter.

We recognize that the FCS eventually fielded will not usually operate independently from other friendly assets. Whereas there is a potential for independent operations, either due to operational necessity or communication failure, it will normally operate within an Objective Force concept. This includes interactions with Joint assets, other FCS-equipped units and allied forces. Within this context, the FCS conceptual design alternatives must account for the transfer of information between the FCS and the Objective Force. We discuss these requirements in this sub-section.

To facilitate this discussion, we introduce the term Objective Force Information Grid, or OFIG. This represents the interface between the FCS and the other friendly assets within the battlespace. We establish this term not to presuppose a client-server hierarchy on the Objective Force network design. On the contrary, we use this term to generalize the source and the recipient of information external to the FCS itself. Our primary purpose for this report is to define the information requirements for the FCS so to properly analyze conceptual design

alternatives. As such, it suits our purpose to represent the assets external to the FCS as the OFIG.

Within each of the BIF there are specific information requirements and responsibilities for the FCS to the OFIG. Below, we briefly discuss some of the significant information flow requirements that support the collaborative engagement process. In appendix A, we provide a table of specific information flow requirements between the FCS and the OFIG. In order to operate and engage collaboratively, the FCS conceptual design alternatives must have the capability to process these information requirements.

3.2.1. Search/Detect

The nature of network-centric warfare is the ability to immediately share information with all other assets in the battlespace regardless of the source of the information. This is especially significant in the Search/Detect BIF. The FCS will indeed have a great deal of organic sensor assets. The information flow between the FCS and external assets will leverage the capabilities of every IO asset in the battlespace.

Without this integration, an FCS will only be able to use their organic assets for searching and scanning. This obviously limits the potentials of this system in a mature theater, but especially limits the capabilities in a situation where we are building forces in a region and limits our operational agility.

3.2.2. Identify

Using the distributed processing capabilities of a network-centric force, we greatly increase our ability to identify entities in the battlespace. Quickly transferring information to the OFIG on the types of entities encountered, the composition of the attacks, if any, and the

capabilities of detected entities all serve to provide insights into the enemy intentions. Coalescing this information obtained throughout the battlespace leads to improved decision-making.

The passing of information between the FCS and the OFIG will greatly reduce our friendly fire engagements and the risk to non-combatants. We can never hope to completely differentiate hostile individuals from non-combatants. The line is very close and differentiation is near impossible. We can however, bring in information on the local populace from higher headquarters, or even national asset, intelligence agencies to assist the on-ground commander. This reach-back capability is essential, especially in a SASO environment.

3.2.3. Target/Track

Information passed between the FCS and the OFIG on targeting and tracking is the true enabler of collaborative engagements between units in the battlespace. Allowing for this, however, enters into Army culture discussions. We address this to an extent in section 4, below.

In our analysis of the FCS conceptual design alternatives, we should not allow this discussion on the suitability of allowing collaborative engagements between dispersed units to limit our capabilities at this point. Overcoming these doctrinal and culture limitations is an issue for future commanders and policy makers. We should concentrate on potentials allowed by NCW. This is a significant potential and must be part of the conceptual design of the FCS.

3.2.4. Engage

The engagement of enemy assets is obviously the essential BIF. The OFIG must report to the FCS unit the engagements made by other assets in the battlespace and the FCS conversely

must report the engagements it conducts. This deconfliction of targets will result in the proper distribution of fires and ensure the minimum expenditure of rounds within the battlespace.

There is also a requirement for the OFIG to dynamically provide rules of engagement and other engagement criteria to the FCS. This will allow for automatic engagements against appropriate target sets. The FCS will also require the capability to adjust the engagement criteria. An example of this adjustment is the encountering of an ammunition bunker. If the engagement criteria directs the destruction of such bunkers, but the system detects the presence of chemical or biological weaponry, the FCS should not engage and then should report this change in status.

Another significant capability the assumption of assets within the OFIG to direct engagements of systems within a FCS in the event the command and control element within the FCS is disabled or otherwise breaks communication with the engaging asset. This requires dynamic resynchronization between the engaging assets and the most local command and control asset available. This does not necessarily have to follow the hierarchical command structure. An adjacent FCS unit may best manage the engaging assets. The system must account for this eventuality.

3.2.5. Assess

Assessment is often an overlooked aspect of any engagement. This is partly due to the difficulty in determining the extent of the damage to the attacked asset. Correct assessment improves survivability and reduces our logistics burden by preventing unnecessary re-engagements.

The significant information requirement passed between the OFIG and the FCS is the knowledge that a successful engagement has occurred. With this information in storage, we prevent a "double counting" of a previously destroyed asset. For example, a unit destroys an enemy tank and then pulls out of that area. A follow-on unit then enters that area and detects a tank hull. Knowledge of the location and composition of the tank directs the computer to determine that there is not threat from this tank and therefore it should not be engaged. When relying on sensors to conduct the search and detect missions, this is a vital information requirement.

3.3. Future Combat System Requirements

In the previous sub-section we discussed the required information to be passed between the FCS and the OFIG. In this section, we focus on the capabilities required within the FCS itself to facilitate the gathering and processing of the information requirements. Below, we explain the individual capabilities required, by BIF. At appendix B, we provide a table that lists the capabilities and delineates specific metrics for each capability. Some of these metrics are binary capabilities. Either the system incorporates that capability into the conceptual design or it does not. Others are numerical and require some measurement. Each should provide some insight into whether a FCS conceptual design alternative is capable of collaborative engagements.

3.3.1. Search/Detect

3.3.1.1. IO assets must be quickly and easily deployable.

The less time and the fewer soldiers it takes to deploy the sensors the better. We cannot assume away the problem of the time and effort involved in getting the right sensor to the right

location, obtaining the correct information from that asset and then, if applicable, returning that sensor asset and preparing it for redeployment. The deployment of IO assets must be made to be a non-labor intensive as possible. This includes the redeployment of these assets, as necessary. Based on the sheer number of IO assets required in a FCS force, tracking them, especially the Unmanned Ariel Vehicles (UAVs) and other robotic sensors will be an overwhelming task. Hence, their deployment and tracking must be specifically addressed in the conceptual designs.

In order to be fully responsive to a rapidly changing battlespace, these IO assets must be deployed quickly from their holding location. For some assets, this may be the back of a host vehicle, whereas for others, it may be in a pod that deploys many assets at once, as in a sensor field. Regardless, there is still a deliberate decision process in the deployment of these assets. By reducing the time required to have IO coverage at a desired location, we allow commanders additional flexibility and responsiveness

3.3.1.2. IO capabilities in deployed systems must be dynamic and adaptive.

By this we mean that the distributed computing capability should allow tracking of IO assets and their coverage throughout the battlespace and either recommend, or autonomously direct, the deployment of additional assets to provide direct or collateral coverage of uncovered zones. The coverage may be degraded for a multitude of reasons. These may include, but are not limited to, destruction, environmental effects, and operational readiness issues. This also highlights problems that arise from varying terrain features, which is the unique challenge the Army faces in implementing network-centric warfare.

The conditions for the Navy and the Air Force are generally the same regardless of the movement of the assets. The Navy has a relatively flat surface to deal with (though there are

special, but rarely changing, conditions for underwater communications). The Air Force generally can maintain line of sight due to the altitude of the planes. The Army must overcome a dynamic battlefield as line-of-sight communications between two assets can be disrupted as a battle progresses[10]. The system must sense this disruption and take immediate action. This can take the form of deploying additional sensor assets, or redirecting loitering assets, or other similar measures.

3.3.1.3. We must employ various types of IO assets.

In a lethal battlefield, such as the one predicted with and FCS-equipped Objective Force, enemy entities can best avoid destruction through detection avoidance. We must be able to counter all methods of detection avoidance through the use of various types of IO assets.

This can be accomplished though the distribution of various types of assets throughout the battlespace and then adjusting those assets upon possible detection. Without trying to direct a design alternative, the force must be able to detect entities through thermal imaging, as a result of movement, through ground vibrations, and using video, to cite a few methodologies. Individually, each of these methods of detection can be easily defeated. When the various types of IO assets are distributed and dynamically linked, however, detection avoidance is near impossible.

Another potential to assist in detection is knowledge of the terrain and the environment. The use of a "reach-back" capability to obtain expert information on the environment in which

---

[10] We acknowledge that the Marine Corps faces a similar challenge to that faced by the Army, but to a lesser extent, under the assumption that the majority of their action will occur in a much smaller Area of Operation (AO) than that potentially faced by the Army. Here, and for the remainder of this paper, we will compare only the Navy and Air Force challenges with that of the Army, as that is the focus of this work, and assume the inclusion of the Marine Corps challenges.

the assets are operating will augment their findings. Anomalies in the environment and/or the surrounding landscape, which are often only noticeable by experts in that region, become useful through distributing the information throughout the battlespace in real time. This capability is only gained through network-centric warfare.

3.3.1.4. IO assets on system must recognize and satisfy dynamic information requirements.

An IO asset does not have to report to its organic host in order to send its message across the battlespace, in all cases. To require such would negate the distinct advantages to be gained from the distributed nature of network-centric warfare. These IO assets must communicate with all other assets available to them. Through the use of distributed and connected computing power, the information gained from an IO asset can be passed throughout the battlespace regardless of the condition of that asset's organic host. This ability will help overcome the limitations inherent in operations in varying terrain and weather conditions, which we spoke of earlier as a unique challenge faced by the Army in network-centric warfare. In the event that the organic host FCS unit is destroyed, damaged or otherwise unable to communicate, the IO assets should continue to report and, if applicable, return to another location for preparation for another deployment. This is a unique approach to equipment and information management, but one that is not only allowed with the advent of a distributed nature of IW, this distributed nature necessitates its implementation.

3.3.2. Identify

3.3.2.1. Must be able to differentiate non-combatants from combatants.

This is difficult and distributed information warfare is no panacea for this critical task. Without some integrated capability, a lighter-weight force directed by the Chief of Staff of the Army, General Eric K. Shinseki, would be either unnecessarily vulnerable to attack from hidden combatants or engaging non-combatants. Neither scenario is desirable.

This capability must be addressed in the conceptual design explicitly. Again, without attempting to direct a design alternative, there are some features of distributed information warfare that could assist in this function. For example, the reach-back capability of a system (the capability to obtain information within the battlespace from outside the battlespace, possibly even from the United States) could assist in identifying traits and mannerisms of hostile actors in a battlespace. Additionally, a design feature could be the capability to detect ammunition, thus identifying combatants. Again, this is a difficult task, but an important requirement, especially with a lightly armored force.

3.3.2.2. Must be able to "mark" enemy/hostile actors.

After differentiating hostile and non-hostile actors in a battlespace, it is not always of military benefit to immediately engage or destroy them. The tracking of these actors could provide insights into enemy intentions and to locations of higher headquarters. It is not always feasible to continuously track these actors, especially in a crowded area. We do not want to reacquire and re-identify these actors. "Marking" them in a passive, unobtrusive manner would alleviate these issues.

3.3.2.3. Must be able to passively identify all friendly assets.

Finally, we must be able to positively identify friendly forces, even when we have limited communications capabilities (such as a power outage or weather anomaly, etc). Again, the vulnerability of the lightly armored force required ease of identification of hostile actors. This is partially enabled by the ability to identify friendly assets. This identification cannot, however, support the enemy's detection of our assets.

The problem of non-passive identification of friendly assets is illustrated by Air Force pilots' reluctance to engage their IFF beacons in a combat environment. Not doing so risks the possibility of a Stinger Anti-Aircraft gunner on the ground not being able to positively identifying that plane as friendly. The reason the pilots do not engage the IFF beacon, however, is the greater fear that the enemy will use that beacon to assist in engaging them! This is an unacceptable situation especially in close combat. Wee must be able to identify friendly assets at all times and it must not put them at greater risk to do so.

3.3.3. Target/Track

3.3.3.1. Must be able to track multiple targets.

There will be numerous targets in the battlespace. We must have the capability to align two or more sensors to each specific target but yet be able to effectively and efficiently track multiple targets simultaneously. Limiting ourselves in this area degrades our ability to engage multiple targets (addressed below). The information gained by tracking multiple targets and their actions provide the necessary knowledge to predict enemy capabilities and their intentions. With the various asymmetric capabilities of an enemy force, we must have this inherent flexibility.

3.3.3.2. Must be able to target and track incoming missiles.

The FCS-equipped system will face a variety of challenges. From a targeting and tracking perspective, the greatest challenge is with incoming missiles, such as a cruise missile. These are relatively inexpensive means by which a rogue nation can quickly inflict great harm on a unit. Through dispersal, the FCS-equipped unit has greatly increased survivability as a system; however, it experiences increased vulnerability as individual platforms. Surviving an attack by either an unguided Scud-like missile or a guided cruise missile is a difficult challenge especially without the guarantee of Patriot coverage.

These missiles may be launched with little or no warning and immediately enter the tracking zone of the FCS-equipped unit. Through the use of this unit's distributed sensor network, however, the missile will, in all likelihood, have an intercept point well past the initial sensor track point. Especially when the tracking sensor capability is linked with satellite and other tracking assets, to include Navy and Patriot assets. Through the use of triangulation and the ability to "pass" the track to other sensors, the missile can be easily tracked and targeted. Without the distributed sensor networks or the ability to pass the target, tracking this missile through a sector would be impossible due to the speed of the missile. The potential damage to a FCS-equipped unit is too great to not require this capability in the system.

3.3.4. Engage

3.3.4.1. The system must be able to engage numerous targets at one time.

As we increase our sensor capabilities, the number of potential enemy targets could increase dramatically. Combine this with the reduced number of friendly assets enabled through distributed dispersed warfare, and the problem becomes attacking many targets within a reduced

timeframe. This drives the requirement for an FCS-equipped force to be able to initiate multiple, simultaneous target engagements.

This demands a system that can fire multiple rounds at various targets. This firing from individual firing platforms can be sequential, as opposed to simultaneous, as the firing can occur from multiple platforms. Regardless, this capability is essential to defeat the multiple threats that this distributed, dispersed force may encounter from a variety of directions.

3.3.4.2. The system must determine the best sub-system to fire and allow firing from other friendly units.

The system will recognize the "optimal" firing system as it has access to information from each system in the entire battlespace. In a platform-centric force, commanders optimize the use of firing platforms locally. By distributing the information capabilities of a force, we can obtain a global optimal solution for the decision on the appropriate firing platform.

There is some resistance to this global optimal firing approach. Commanders are reluctant to allow others in the battlespace to fire "their" ammunition. The promise that the decision to fire their ammunition is based on the benefit to the force as a whole is of little condolence as their sense of capability to defend themselves against direct enemy engagements is reduced. Though these are legitimate concerns of commanders, they cannot persuade us to globally optimize firing throughout the battlespace.

This capability extends beyond the reach of a FCS-equipped unit, regardless of the size of that unit (brigade-, battalion- or company-equivalent). This capability must extend to Joint as well as non-FCS-equipped units. The firing from non-FCS-equipped units may be via direct, even voice, communications, but the capability must still exist. Sensors allow and FCS-equipped

force to engage an enemy force in a traditional call-for-fire mission without having actual "eyes on" the target. This capability must still exist between assets.

3.3.4.3. The systems must engage in manual and in automatic modes.

The system should be able to direct engagement of targets, but it is not always beneficial to allow the system to automatically conduct that engagement. There are always considerations inherent in a dynamic battlespace that are best left to a commander, or executer, on the ground. There must be a capability for the system to recommend a engagement option while allowing the commander to choose another system recommended option, or even an entirely different option. This includes the option to not engage the entity.

This capability can be likened to a pitcher-catcher relationship in baseball. In baseball, the catcher recommends the best option to the pitcher through signals. It is the pitcher, however, who possesses the "feel" of which pitch he has the best command of in a given situation. He has the ability to "shake off" the recommended pitch-type and choose something else. In the end, the pitcher has the final decision, as well as the responsibility for the result. The same is true in combat with commanders. Distributed information warfare allows commanders and other engagers to receive recommendations as to the global optimal solutions, but the final decision must be theirs. The system must then automatically adjust other recommendations throughout the force as individual commanders modify the objective criteria.

3.3.4.4. There must be a direct fire and force protection system.

In spite of the advanced capabilities of sensors throughout the battlespace, there will always be the potential threat to any system from close combat. This may be in the form of "pop-up" enemy targets that have laid in wait for the system, or due to the rapid closure of the

system onto an objective. This threat can also take the form of an asymmetric, guerrilla-like attack during a time of reduced vigilance, such as in a night cantonment or during resupply operations. Regardless, without the capability to defend itself from soft targets, the FCS-equipped force will be vulnerable to these threats.

There is some contention as to the nature of this direct fire "surprise" force. It is possible that it could be armored, but is more likely to be soft, unarmored individuals. The basis of this contention is two-fold. First, sufficiently hiding a large armored entity from the entire suite of sensors in an FCS-equipped battlespace will be extremely difficult. Second, in the event some armored threat does enter the FCS-equipped force's direct fire range, the entity can be engaged through either indirect, or BLOS fires from organic, or collaborative assets.

The greater likelihood is attack from guerrilla-like ground forces using small arms, armor-piercing rockets or missiles, or other explosives. This likelihood, however remote, is significant in the damage it may inflict. For this reason, there must be a capability to passively identify and quickly attack these threats. The reduced detection inherent in these close threat assets, as well as the reduced flight time of missiles and rockets, directs the use of on-board assets to eliminate them. Indirect, or BLOS, actors cannot effect the threat in sufficient time to defend the system, or the individual platform. We limit our discussion here to infiltration attacks and in the next section we address missile attacks.

The system must have a capability to provide force protection and in both the manual and automatic modes to defend against this infiltration threat. During the times of potentially reduced vigilance and vulnerability, the system must be able to sense and direct fires with on-board systems.

3.3.4.5. There must be an anti-missile capability.

Engaging a missile requires a much different warhead capability than engaging a tank or a soft target. Due to the relatively low cost of production and acquisition and the proliferation of the cruise missile technology there is a realistic threat to the FCS-equipped Objective Force from this type of attack. This includes the threat from cruder, but potentially equally effective Scud-type missiles. We cannot rely solely on the availability of Patriot coverage throughout the battlespace to counter this threat. This threat can be countered using the collaborative engagement capabilities inherent in the distributed force.

Some other missiles, however, cannot be addressed through collaborative engagement capabilities. There is also a real threat from a "pop-up" anti-tank rocket threat again due to the low cost of these launchers and the ability to hide their presence. The potential for multiple launches of these rockets from different locations on a given target increases the difficulty in counter this threat. Due to the low flight time of these attacks, defending against them must be done through on-board systems. These on-board systems are absolutely necessary on manned systems. Unmanned systems are important, but due to the collaborative and redundant nature of the FCS-equipped force, their loss is not as detrimental to the capabilities of the overall system.

3.3.5. Assess

3.3.5.1. Feedback on BDA must be immediate.

With a lightly armored vehicle, such as a proposed FCS system is likely to become, successfully engaging the enemy before he can do so to you is a matter of life or death. In such an instance, we cannot wait to determine if an engagement is successful very long as we have to err on the side of too many shots versus not enough. Similarly, if we ever hope to reduce logistics by achieving a greater than one round per stowed kill (as TRADOC suggests as a goal),

we cannot expend unnecessary ammunition at enemy entities we have already successfully engaged.

3.3.5.2. The system must be able to determine level of damage and remaining capability of attacked system.

Determining the level of damage to a enemy system is a matter of knowledge of the system and what defines a sufficient level of damage. For example, an enemy tank may be a mobility kill, but still be able to fire a round. In this case, defining a successful engagement as a tank that no longer moves would be insufficient. This capability is best gained through a combination of the use of multiple types of sensors and a distributed processing, or even reach-back, computing capability. This will provide the most updated assessment of the best interpretation of the information from the dispersed, varied types of sensors.

3.3.5.3. System should automatically update database with damage information.

This seems logical as the overall system should be updated with all information at all times, but it is crucial that we positively track damage to enemy entities we have engaged. Failure to do so will result in either an enemy being re-engaged even though we have previously successfully engaged or, worse yet, not being engaged and being allowed to move freely within our lines.

3.4. Summary

In this section, we have looked in great detail at the five BIFs that provide the framework for the analysis of the FCS conceptual design alternatives. We have also identified the changes in these functions brought about by distributed information warfare. Finally, we have identified

some significant metrics within each capability that could be used to measure the effectiveness of the conceptual design alternative to achieve that capability.

We have focused our discussion of the analysis of the FCS conceptual design alternatives on these BIFs with a specific rationale. The ability to leverage these BIFs through distributed information warfare will allow us to achieve the RMA we seek through NCW. This should be the focus of our analytical treatment of the conceptual design alternatives. These BIFs should also be the focus of our research and development programs. It is here that we will find the RMA we seek.

We do not intend to suggest that this framework should be the only considerations for the FCS conceptual design alternative analysis. There is, for example, a definitive deployment threshold established by the Army Chief of Staff that a brigade-sized unit must be on the ground, ready to fight, in less than 96 hours. This is a critical measure for any conceptual design. It must be considered and evaluated. It, however, becomes a screening criterion. In that we mean, that if a conceptual design does not make this threshold, it should be eliminated. If it does, then it should be accepted for further evaluation. Evaluating a concept higher based solely on the basis of a quicker deployment capability will not give us the leap in capability we seek as there is no RMA present in the deployment process at this time. There may be in the future, but we should not focus our analysis here at this time.

Most frameworks for analysis to this point have focused on the "-ilities". This is an admirable approach, but it is limited as it provides no operational framework nor does it help focus our analysis. Most of the "-ilities" are represented within the framework we propose. For example, lethality and survivability are both directly considered within this framework.

Flexibility and adaptability are more influenced by organizational and doctrinal constructs and should be left for that portion of the analysis.

Mobility is much like deployability. It is extremely important, but as there is not RMA found within this area, focusing our analysis here will not lead to the leap in capability we seek. There is a potential for an RMA in this area, however. The operational mobility of a force can provide a leap in capability similar to that of the fielding of the gas engine and the railroad. We are not at the point yet in technology however to move an entire force quickly enough to wage war in a revolutionary manner. This can be achieved through the development of a hovercraft, vehicles that can operate on the ground as well as in the air for even short periods, or even a distributed force that can reconfigure into one entity, lift off using organic assets and then decouple. Until this capability is better defined and more realistic, however, we should not turn our attention away from the current RMA we face and focus on evolutionary mobility gains.

There has been some discussion of a Revolution in Logistics Affairs (RLA). We are not to that point however. Just-in-time logistics will improve the existing re-supply concept, but it does not change the way we currently provide for the force – especially in light of the recent criticism of this approach. Until we can change the huge reliance on fuel and ammunition resupply, we cannot fundamentally change this operation. Reducing the burden through improved gas mileage, more precision engagements and improved reliability will greatly improve the logistic operation, but will not change it.

The focus of this report is simple. The force that can collectively engage the enemy through distributed information warfare will attain the RMA and dominate the battlespace throughout the first half of this century. We must focus our analytical efforts to ensure the

conceptual design alternatives have this capability. Focusing our efforts elsewhere may provide us with an evolutionary solution. If we do not push the community with requirements and/or funding to make these technologies a reality, we will miss this opportunity. We must remember what the Polish Horse Cavalry soldiers thought of their military development community when they saw the first wave of the German *Wehrmacht* employ their tank-led *Blitzkrieg*. We must do better.

A significant part of our ability to exploit the BIFs is a review of our doctrine to determine what could and what should change in order to take advantage of our new capabilities. Using these capabilities within existing doctrine would unnecessarily restrict the effectiveness of the FCS-equipped Objective Force. In the next section, we identify some areas that we should review within our doctrine for potential changes.

4. Doctrinal Innovations

Returning to our definition of a RMA, we note that the second precondition is associated doctrinal innovation that employs technological advances in novel and significant ways. We do not propose changing our successful doctrine for the sole purpose of achieving a RMA. However, we can state unequivocally that without some innovative changes in our doctrine, we cannot fully leverage the potentials of collaborative information warfare.

In this section, we attempt to quickly review some aspects of our doctrine that we should consciously review for potential changes. These changes concern fire control measures, span of control within organizations and the information requirements that will support flexible organizational structures. These proposals are intended to lead to more in-depth discussions. Some of the significant, necessary changes to command and control in a distributed information warfare environment deal specifically with leader training and development issues, which we leave for another study.

4.1. Fire Control Measures

For over 40 years, our doctrinal discussions focused on the Soviet threat in Eastern Europe. In this battle that never occurred, we envisioned an almost "organized" type of warfare. The lines were clearly drawn, the enemy was very distinguishable and the friendly forces were to move as if lead by a prima ballerina. The fighting would be violent no doubt, but we could use distinct fire control measures such as unit boundary lines to control the fires and movements of friendly forces.

In this situation, commanders controlled the action within their boundary lines, or their *sandbox* as it was often referred to. One could not fire across unit boundary lines unless it was coordinated ahead of time. A unit could not move across a boundary line without coordinating that action. Orders were written to time fires and ensure the "weighted effort" received priority support for artillery fires. A linear battlefield with a very open, distinguishable enemy lent itself to this type of control measures. A non-linear battlefield does not.

In a non-linear battlefield, the friendly forces could be directly in the middle of an enemy force and have to fight in all directions. We may have some FCS-equipped forces moving east while others move to the west, or any other direction. The "best" shot at a enemy directly in front of unit may be the one taken by a friendly unit 20km away. We have the capability now to allow collaborative engagements from all friendly entities on the battlefield. We must encourage this type of engagements and not be tied to the notion that we cannot fire into someone elses sandbox. We need to get away from everyone individually fighting the best fight they can in their area and move to the time when we can collectively fight the best fight the entire force can fight. We can only do this by changing our mindset on controlling fires through boundary and phase lines and allowing collaborative engagements between units.

4.2. Span of Control

This is a difficult subject as it moves into a discussion on human factors and out of the realm of pure military doctrinal analysis. It is a long held notion that a human can best manage 3-5 entities. This is the prime rationale for battalions having 3-5 companies and platoons having 3-5 squads. Faced with more, and the human will be ineffectual; less and be under utilized. A shift to a more autonomous sub-system like the FCS may challenge that premise.

As the tracking of the locations of all subordinate units and their status will be automatically updated in near real time through the network, there will be less specific "management" of most trivial aspects of command. There will be potential for further automation of some additional command functions. All this may lead to an opportunity to eliminate, or modify, entire levels of command. Even now, there is some discussion of not requiring only battalions and not brigades within a division structure. We should explore this potential to the greatest extent. The reduction in personnel and equipment overhead through this type of innovation would be tremendous. This alone would justify the shift to an FCS-equipped force.

4.3. Flexible Organizational Structure

The FCS-equipped force is being designed to fight across the spectrum of warfare and to quickly transition from one type of conflict to another. Additionally, these forces may be required to quickly add subordinate FCS units of action to higher headquarters. This may take the form of additional units entering a theater of operations or additional augmentation of forces for a specific phase of an existing operation. To obtain this flexibility we must design into our systems the ability to rapidly pass the necessary information about the augmented unit to the higher headquarters as well as the higher headquarters passing the appropriate operational information to the augmented unit.

Whereas on the surface this information-passing requirement may seem like a design requirement, this becomes a doctrinal issue, as we must analyze the information required to facilitate this augmentation. Some of the higher headquarters information requirements are the composition of the augmented unit in terms of personnel, equipment, capabilities and logistics

status. Some the augmented unit requirements are the operational plan of the higher headquarters, the command structure and the capabilities of the other subordinate units within the new command.

Though our current doctrine allows for changing the task organization of a force, without the capability to seamlessly, efficiently and effectively transfer units of action between higher headquarters, we reduce the potential flexibility of our operational units. This will also allow us to more quickly establish a task force organization to accomplish a specific mission such that previously proposed by MacGregor and Kragen (1997) and others.

4.4. Summary

Undoubtedly, there needs to be changes in our doctrine upon fielding of the Objective Force. We cannot change the way we attack an enemy and not re-look some of our current doctrinal procedures. Fortunately, there is a great deal of discussion in this area already. This short list we propose here is only a start of the re-look we will be required to analyze. Maintaining our current procedures will reduce the stress on the force brought by changing the equipment, but it will not provide us with the leap in capability that we seek or require on the future battlefield.

5. Organizational Acceptance

Of the three preconditions of a RMA, the final precondition, organizational acceptance, may be the most difficult to obtain. Changing the inertia of a successful organization is extremely difficult, more so with an organization as large as the Army. With a backdrop of the success of Desert Strom, there is a culture change required prior to any acceptance of a dramatic change in equipment and procedures. We must be able to prove to the military community and to Congress that the FCS is better in every way from our previous capabilities and justifies the expense involved. To accomplish this, we issue two mandates to the analytical community.

Our first mandate is to the Modeling and Simulation community. They must appropriately and completely model new systems (under design), specifically the distributed collaborative information operations capability envisioned by the Objective Force designers. Simulation efforts to date have focused on modifying current, attrition-based simulations to account for the passing of information. This is insufficient to properly demonstrate the envisioned exponential increase in information operations, which enable the Objective Force capabilities. To this point, simulations have been developed to follow the operational organization, which does not allow the Defense community, and Congress, to fully appreciate the potentials of the new systems. We must change this paradigm.

The second mandate is to the analytical and academic communities. These resources must address the specific capabilities of the Objective Force and detail how to achieve those capabilities. This will serve to reduce the speculation and supposition that typifies current operational discussions and reduces confidence in the success of the initiative. In addressing the

shortcomings of the efforts of the analytical community in the development of the capabilities of a tank force in 1937, Liddell Hart stated:

> The more one examines the course of past wars the more one is impressed by the frequency with which military policy and preparations have taken the wrong turning. And this abnormal percentage of error can be traced to the habit of basing policy and preparations on an assumption, without adequate verification. The way that decisions are reached on questions of strategy, tactics and organization, etc. is lamentably unscientific. It is due in part to the difficulty of developing a truly critical habit of mind under the conditions of military subordination, and in part to the lack of any staff organ devoted to research (Hart, 1944).

Without the input of analytical thinking directed specifically at the development of the Future Combat Systems from the academic arm of the military research community, namely the Army War College, the Institute for Defense Analysis and others, we run the risk of missing the true nature of this revolution. These analytical organizations must enter into the fray on this development of the FCS immediately and continuously to convince the Defense community and Congress of the eventual success of the overall program.

6. Summary and Conclusions

In this technical report, we have proposed a framework for analyzing the conceptual design alternatives for the Future Combat System (FCS). We started with the premise that if we are to fully leverage the potentials of a network-centric environment, we must seek the change that will provide us with a Revolution in Military Affairs (RMA). We do not seek a RMA simply to give historical significance to the Objective Force effort. Rather, we seek the RMA to provide us with the greatest increase in operational capability. As we stated previously, an RMA requires three preconditions: first, a fundamental change in the nature of warfare, second, doctrinal innovations, and third organizational acceptance.

The accomplishment of each of these preconditions is essential to the overall success of the Objective Force program. Some advocates of other aspects of the Future Combat System will attempt to sidetrack the discussion to support their positions. Here we have established the groundwork for an on-going analysis effort. Our timeframe is short and the challenge formidable. The consequences for the future of our Army, however, are dramatic.

References

Alberts, David S., John J. Garstka and Fredrick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, (2000) 2nd ed, CCRP Publication series, DoD C4ISR Cooperative Research Program, Washington, DC.

Arquilla, John, "The 'Velvet' Revolution in Military Affairs," World Policy Journal, (Winter 1997/1998): 35.

Bazaraa, Mokhtar S., Hanif D. Sherali and C. M. Shetty, *Nonlinear Programming: Theory and Algorithms*, (1993) 2nd ed., New York: John Wiliey & Sons, Inc.

Clancy, Tom, *Armored Cav*, (1993), New York: Berkley Books, p. 254-258.

"Cooperative Engagement Capabilities", Applied Physics Laboratory, (1995), Johns Hopkins APL Technical Digest, Volume 16, Number 4.

Correl, John T., "Signs of a Revolution", *Air Force Magazine*, (1995) editorial vol. 78, no. 8.

Department of the Army Field Manual 17-12-1-1, "Tank Gunnery (Abrams) Volume I – Tank Crew Handbook", Washington, DC, 5 May 1998

Development and Readiness Command (DARCOM) Pamphlet, 706-101, "Engineering Design Handbook – Weapon Systems Analysis, Part One", Department of the Army, November 1977, p 11-9.

Eisenhower, Dwight D., *At Ease: Stories I Tell to Friends*, (1967), 1st ed., Garden City, New York: Doubleday and Company.

Ellis, John, *The Social History of the Machine Gun*, (1975), Baltimore: Johns Hopkins University Press.

Fitzsimmonds, James, R., and Jan M. Van Tol, "Revolutions in Military Affairs," Joint Forces Quarterly, (Spring 1994), 4, pp. 24-31.

Hart, Liddell, *Thoughts on War*, (1944), London: Faber and Faber, Ltd.

Hoyt, Edwin P., *Carrier Wars: Naval Aviation from World War II to the Persian Gulf*, (1989) New York: McGraw.

MacGregor, Douglas A., Breaking the Phalanx: A New Design for Land Power in the 21st Century, (1997) Westport: Praeger Publishing.

Marshall, Andrew W., "Revolutions in Military Affairs", Director of the Office of Net Assessment, Statement prepared for the Subcommittee on Acquisition and Technology, Senate Armed Services Committee, 5 May 1995, p.1.

Murray, Williamson, "Thinking About Revolutions in Military Affairs," Joint Forces Quarterly, (Summer 1997), 16, pp. 69-76.

Naval Studies Board, *Network-Centric Naval Forces: A Transition Strategy for Enhancing Operations Capabilities*, (2000), Washington, DC: National Academy Press.

O'Hanlon, Michael, *Technological Change and the Future of Warfare*, (2000) Washington, DC: Brookings Press.

Parker, Geoffrey, *The Military Revolution: Military Innovation and the Rise of the West* (1998) Cambridge, Great Britain: Cambridge University Press.

Scales, Robert H., *Future Warfare: Anthology*, US Army War College, Carlisle, PA.

Shinseki, Eric K., Address to the Eisenhower Luncheon, 45th Annual Meeting of the Association of the United States Army, October 12, 1999, Chief of Staff, Army.

Rogers, Clifford J., "The Military Revolutions of the Hundred Years' War," in Clifford J. Rogers, ed., The Military Revolution Debate: Readings on the Transformation of Early Modern Europe (1995) Boulder, CO: Westview Press, 55.

Rothenberg, Gunther E., *The Art of Warfare in the Age of Napoleon* (1978) Bloomington, IN: Indiana University Press, 1978, 11.

Welch, Thomas J., "Revolution in Military Affairs: One Perspective" in Strength Through Cooperation: Military Operations in the Asia-Pacific Region, (1995) eds. Frances Omori and Mary A. Sommerville, on-line books, National Military Defense University.

Appendix A: Future Combat System and Objective Force Information Grid Requirements

	FCS Information Requirements	
Battlefield Information Function	**FCS provides Objective Force Information Grid (OFIG) with information on:**	**Objective Force Information Grid (OFIG) provides the FCS with information on:**
Search/Detect	Locations searched by organic assets with negative detections, type of sensor asset utilized and time of most recent search. Location and activity of entities detected by organic assets. Capabilities, location and coverage of deployed ground-based sensor networks. Capabilities, location and coverage of deployed aerial sensor networks. Capabilities, location and coverage of deployed robotic sensor networks. Capabilities of non-deployed sensor assets. Limitations of sensor coverage. Presence of NBC threat Presence of man-made obstacles and structures Results from search requests	Locations searched by non-organic assets with negative detections, type of sensor asset utilized and time of most recent search. Location and composition of entities detected by non-organic assets. Joint and National asset data collections. Capabilities, location and coverage of deployed ground-based sensor networks. Capabilities, location and coverage of deployed aerial sensor networks. Capabilities, location and coverage of deployed robotic sensor networks. Capabilities of non-deployed sensor assets. Limitations of non-organic sensor coverage Presence of NBC threat Type and composition of man-made obstacles and structures Search requests

	FCS Performance Capabilities	
Battlefield Information Function	**FCS provides Objective Force Information Grid (OFIG) with information on:**	**Objective Force Information Grid (OFIG) provides the FCS with information on:**
Identify	Location and activity of system platforms. Location and activity of dismounted soldiers. Location and activity of aerial assets. Type of attack on organic sub-systems. Non-combatants identified within battlespace. Type and location of NBC threat Type and composition of man-made obstacles and structures Location and of encountered friendly assets Marking of friendly, enemy and non-combatant entities Results from request for identification or validation	Non-organic dismounted friendly assets within the battlespace. Non-organic mounted friendly assets within the battlespace. Non-organic aerial friendly assets within the battlespace. Dismounted enemy assets within the battlespace. Mounted enemy assets within the battlespace. Aerial enemy assets within the battlespace. Non-combatants identified in battlespace. Indigenous population within the battlespace. Capabilities and tendencies of suspected enemy forces. Type and location of NBC threat Type and composition of man-made obstacles and structures Requests for identification or validation

	FCS Performance Capabilities	
Battlefield Information Function	**FCS provides Objective Force Information Grid (OFIG) with information on:**	**Objective Force Information Grid (OFIG) provides the FCS with information on:**
Target/Track	Targeting and tracking incoming missiles with organic assets. Targeting and tracking dismounted entities with organic assets. Targeting and tracking mounted entities with organic assets. Surveillance information on marked entities	Targeting and tracking missiles with non-organic assets. Targeting and tracking mounted entities with non-organic assets. Targeting and tracking dismounts outside its battlespace. Potential enemy courses of action. Request to conduct surveillance operations on marked entities

	FCS Performance Capabilities	
Battlefield Information Function	**FCS provides Objective Force Information Grid (OFIG) with information on:**	**Objective Force Information Grid (OFIG) provides the FCS with information on:**
Engage	System notifies OFIG of targets it engages. System engages entities targeted by non-organic assets. System provides information on its organic engagement capabilities. System adjusts and reports engagement criteria	System receives information on targets engaged by other friendly entities. System receives information on engagement capabilities of other friendly entities. Rules of Engagement Dynamic alteration of engagement criteria Remote engagement orders

	FCS Performance Capabilities	
Battlefield Information Function	**FCS provides Objective Force Information Grid (OFIG) with information on:**	**Objective Force Information Grid (OFIG) provides the FCS with information on:**
Assess	Location of previously engaged entities that are assessed with organic assets. Capability of previously engaged entities to move Capability on previously engaged enemy to shoot Capability of previously engaged enemy to communicate Reports on requests for assessment of identified assets	Location of previously engaged entities that are assessed by non-organic assets. Capability of previously engaged entities to move Capability on previously engaged enemy to shoot Capability of previously engaged enemy to communicate Requests for assessment of identified assets

Appendix B: Future Combat System Requirements

Search/Detect	**Metric**
Deployability of I/O assets	• Time required for sensor assets to be operationally capable after deployment decision • Personnel required to deploy sensor assets • Personnel required to monitor sensor assets • Personnel required to redeploy sensor assets • Time required to redeploy/recover sensor assets • Number of I/O asset deployments available without resupply
Dynamic and adaptive I/O assets	• Sensor assets report reduced capabilities • System identifies lapse in reporting from sensor assets • Sensors assets dynamically report assets other than host vehicle/unit, as required
Types of I/O assets employed	• Sensor assets can operate in adverse conditions • Number of types of I/O assets available
Operation of I/O assets	• Percentage of dismounts detected in urban terrain • Percentage of mounted assets detected • Percentage of aerial assets detected • Cubed volume of sensor coverage • Duration of sensor coverage • Granularity of data • On-board integration of sensor data • Direct communication between sensors and data integration centers

Identify	Metric
Differentiation of combatants and non-combatants	• Percentage of combatants properly identified • Percentage of combatants improperly identified as non-combatants • Percentage of non-combatants improperly identified as combatants • Time required to differentiate combatants and non-combatants
Marking of enemy/hostile actors and non-combatants	• Percentage of enemy/hostile actors requiring re-identification • Time required to identify enemy/hostile actors
Identification of friendly assets	• Time required to identify friendly assets • Percentage of friendly assets requiring re-identification • Emissions by friendly assets required for identification • Ability to passively re-establish the identity of friendly assets

Target/Track	Metric
Track and target multiple enemy entities	• Number of enemy ground and aerial entities tracked simultaneously • Number of enemy ground and aerial entities targeted simultaneously
Target and track incoming missiles	• Number of incoming missiles tracked • Number of incoming missiles targeted

Engage	Metric
Engage multiple targets simultaneously	• Number of potential targets engaged in given timeframe • Number of engagements possible without resupply • Time required to resupply for subsequent engagements
System provides recommendations for firing platform and ammunition.	• Number of recommended firing platforms per target set • Number of dismount targets potentially engaged • Number of armored/bunkered targets to be engaged • Time required for recommendation • Time from decision until execution of mission
System engages in manual and automatic modes.	• Time required to engage in automatic mode • Percent of correct engagements in automatic mode • Time required to engage in manual mode
System has direct fire capability	• Number of direct fire engagements possible • Number of platforms with direct fire capability • Range of direct fire weaponry

Assess	Metric
Immediate Battle Damage Assessment	• Time required to assess damage after engagement • Percentage of proper assessments after engagement
Remaining capability assessment	• Percentage of correct mobility assessments • Percentage of correct firepower assessments
Database updated	• Time required to update database